The process 10 first initializes the handheld computer 3 (step 50). The process then selects a file associated with the current project and brings up the data on screen (step 52). Next, the user performs the civil field inspection (step 53). During this process, the user can use the sketchpad to sketch potential problems or simply to annotate comments (step 54). The user can also send comments and revisions to the service providers based on the progress and the costs. Alternatively, all parties can teleconference over the Internet or over conventional telephone connections (step 55). Alternatively, the user can capture an image or a video of the construction project using the camera (step 56).

If the handheld computer 30 includes a wireless modem, periodically, the service providers upload text annotation, sketch annotation, individual images or video clips of the construction progress to the server (step 58). The images can be compressed using an industry standard format such as JPEG or GIF, while the video clip can be compressed using MPEG, among others. Alternatively, other techniques such as sound bites describing a walk through of the remodeling progress can be uploaded in lieu of the images or video clips.

Fig. 1B shows a process for viewing the data uploaded by the handheld computer 30 to the server 20. A user such as a project manager can periodically log-on to the server to view the progress of the construction (step 60). The images may be played one at a time (step 62) or in sequence to show a movie detailing the construction progress (step 64).

Fig. 2 illustrates an exemplary hardware configuration system 110 for executing the modules of Fig. 1. In the system of Fig. 2, one or more mobile computers 112, 114 and 116 are carried by one or more inspectors. The mobile computers 112, 114 and 116 are connected to a dialup network 120. The data transfers can be performed using this dial-up network or directly from local area network at the main office. Specifically, the dialup network can simply be the Plain Old Telephone Service (POTS) network. Each mobile computer executes

a field inspection software that communicates with a camera coupled to the computer to capture video, a sketch pad coupled to the handheld computer to capture a sketch. Each mobile computer also contains code to communicate the video and sketch with a remote user such as a project manager.

The dialup network 120 in turn is connected to a server 130 which is protected by a firewall. The firewall is a security system (hardware and/or software) that isolates resources of a computer system or network from objects outside of the system or network. Generally, the firewall allows for inside objects to request and receive connections to outside objects (e.g. for inside applications to access outside Internet sites, among others), but prevents outside applications from accessing resources inside the system or network.

Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the Email service. Other firewalls provide less strict protections, and block services that are known to be problems. Generally, firewalls are configured to protect against unauthenticated interactive logins from the "outside" world. This, more than anything, helps prevent vandals from logging into machines on the user's network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside.

The server 130 is connected to one or more contract databases 132, 134, 136, and 138. The server 130 also is connected to a master server 140. The master server 140 is connected to one or more master databases 142, 144, and 146. The master server 140 is also connected to one or more workstations, including a project manager workstation 150, a project engineering workstation 152, and an estimator workstation 154.

In this implementation, the master server 140 can be a plurality of redundant, fail-over servers, where each server can provide resources independent of the other until one of the

servers fails. Each server continuously monitors the other server. In one implementation, server processes available from Microsoft Corp. of Redmond, Washington called Microsoft Cluster Server (MSCS) uses a hot-standby technique in which a primary server and a standby server send "keep alive" messages back and forth so that the standby server is activated if it cannot contact the primary server. When one of the servers fails, the surviving server acquires the shared drives and volumes of the failed server and mounts the volumes contained on the shared drives. Applications that use the shared drives can also be started on the surviving server after the failover. Further, a manual-failover operation can be performed on the shared volumes at any time in order to perform tasks such as scheduled maintenance on one of the servers. As soon as the failed server is booted up and the communication between servers indicates that the server is ready to own its shared drives, the servers automatically start the recovery process.

The databases 142-146 can reside on one or more network RAID data storage devices. In such an embodiment, the network RAID data storage device is a collection of disks under hardware or software control so that a single drive failure does not bring the system of Fig. 1 down. The data storage devices may be a RAID-1 system, in which every disk has a mirror image of its data stored on another disk. Alternatively, the data storage devices may be a RAID-2 or RAID-3 sub-system which stripes user data across a group of data drives (typically four or eight drives per group). The data storage devices may also be a RAID-4 or RAID-5 sub-system which stripes block (or sometimes groups of blocks) of data and stores the data entirely on an individual disk.

Referring now to Fig. 3, major modules associated with the system of Fig. 2 is shown. In Fig. 3, a field journal 162 is maintained on an inspector portable computer 164. The